

五問您的 DDoS 緩解服務提供者

隨著 DDoS 攻擊頻率和複雜性的加劇，選擇合適的 DDoS 緩解服務對於保護您的網路和使用者來說至關重要。然而，並非所有服務都生來平等，選錯服務可能會導致意想不到的麻煩、效能問題和停機時間。

在評估 DDoS 緩解服務提供者時，您應該考慮下面五個問題：

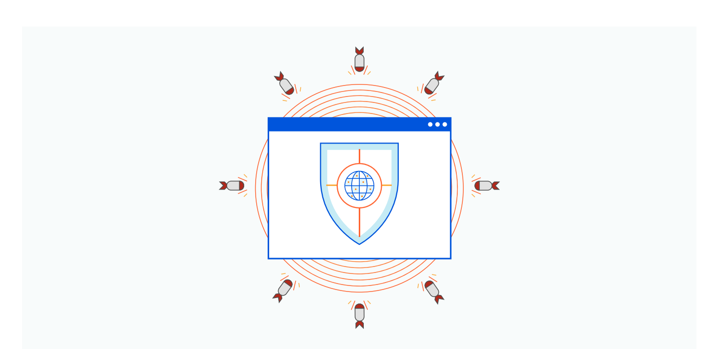
1. 服務是雲原生的嗎？

DDoS 緩解服務若要發揮效用，必須是雲原生的，不能是經過虛擬化並託管於雲端資料中心的本地部署技術。有何區別？雲原生緩解服務可以根據您的業務需求無縫擴展，不會造成人為的效能瓶頸，而雲託管虛擬裝置仍然具有與本地硬體相關的管理複雜性。



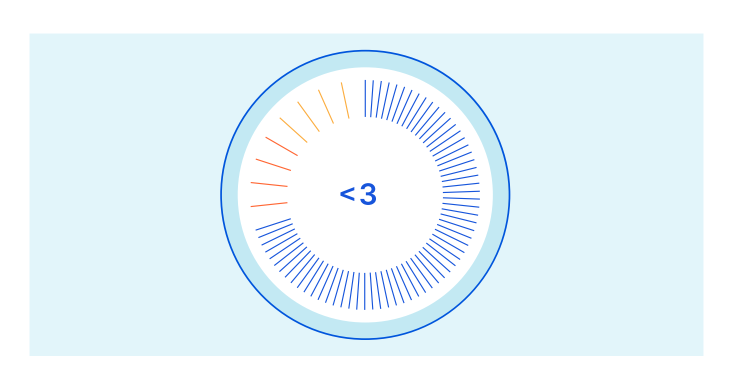
2. 提供者提供的網路處理能力有多大？

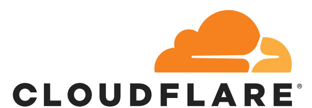
大規模 DDoS 攻擊 (例如 2020 年針對 AWS 客戶的2.3Tbps 攻擊) 可能會使網路處理能力不足的服務提供者不堪重負，無力吸收 DDoS 流量。若要對抗這種規模的攻擊，您要選擇提供充足網路處理能力的提供者，從而既能抵禦攻擊，也不會導致停機或效能下降。



3. 服務可以多快速度偵測和回應 DDoS 攻擊？

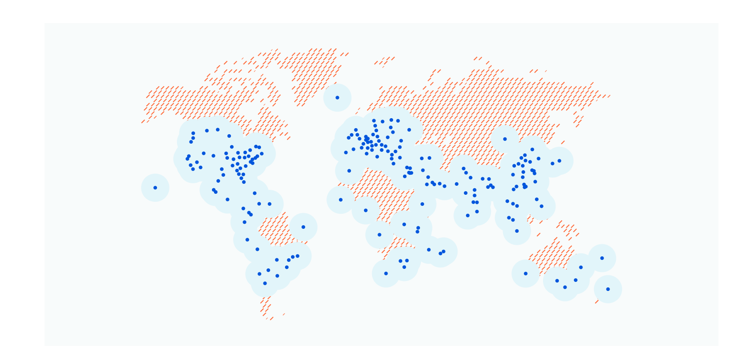
面臨攻擊時，較短的緩解時間 (偵測和緩解攻擊所需的時間) 至關重要。停機時間一旦超過幾秒鐘，就會給客戶體驗、品牌聲譽和收入造成不可逆轉的損害。





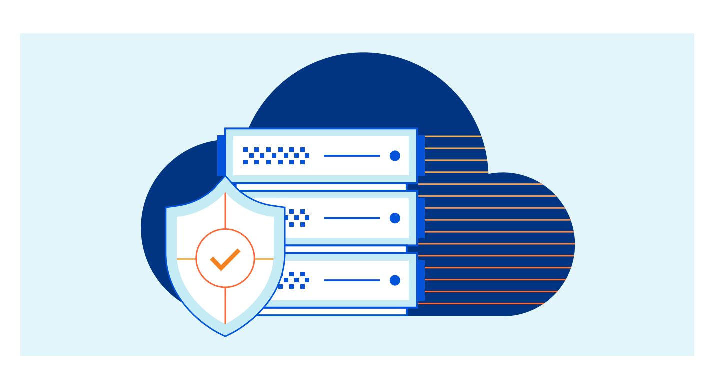
4. 服務是否在每個資料中心都可用？

如果做不到 DDoS 清理功能在每個資料中心均可使用，您的流量將不得不透過專門的「清理中心」返回，這通常會增加延遲並影響應用程式效能。選擇可在每個資料中心提供緩解服務的提供者，同時將您的流量保持在最佳路徑上。



5. 服務是自動化的嗎？

強大的 DDoS 緩解服務應透過儀錶板或 API 提供自動化和自助服務能力，讓您能夠快速開啟和管理威脅防護。您要尋找的提供者必須易於聯絡，回應快速，主動偵測和緩解威脅，並且對您的服務停機時間沒有任何影響。



Cloudflare Magic Transit 可保護整個 IP 子網免受 DDoS 攻擊，同時還可加速網路流量。Cloudflare 的全球網路 (覆蓋 200 多個位置的資料中心) 每天平均封鎖 700 億次威脅，包括史上規模最大的一些 DDoS 攻擊。

要開始使用 Magic Transit，請立即申請免費演示。